SYSTEM AND METHOD FOR CONDUCTING SECURE TRANSACTIONS OVER A NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application No. 60/255,004 filed December 12, 2000, the entire disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0001] The present invention relates to conducting secure transactions over a network. In particular, the present invention relates to a system and method for conducting secure transactions over a network in which the identity of a party to the transaction is verified.

[0002] Computer networks, such as the Internet, are used for a variety of commercial activities, such as banking transactions, stock trading and the purchasing of goods and services. The Internet in particular provides a vast new market, and significant new opportunities, for a wide variety of businesses.

[0003] A common method for conducting business transactions over the Internet, or over other computer networks, is to use a credit card to authorize and pay for the goods or services. A consumer, typically using a personal computer, cell phone, personal digital assistant (PDA) or other communications device, electronically connects to a provider of the goods or

services. Using browser software, the consumer then reviews the provider's website, selects particular goods or services for purchase, and then provides personal and financial information to complete the transaction. Completing the transaction typically involves entering a name, address, credit card number, credit card expiration date and other information pertinent to the transaction. The consumer usually enters this information using a keyboard, mouse or other input device associated with the communications device. The provider typically requests credit authorization from an authorizing entity, such as a credit card company or bank, and, if such authorization is provided, the transaction is completed.

[0004] While this method is effective, it is subject to abuse and fraud. According to recent newspaper articles, the theft of information associated with a person's identity, such as a person's social security number, credit card number, driver's license number or passport number, has become a major problem. In particular, the theft of a person's credit card number is causing significant losses to providers of goods and services over the Internet. For example, in 1999, providers of goods and services over the Internet lost approximately 230 million dollars in revenues because of credit card fraud. Reducing such fraud is an important goal to the future of the Internet.

[0005] The use of biometric devices, such as fingerprint analyzers, iris scanners, etc., is known for verifying a person's identity. Biometric devices are not widely used for transactions with consumers, however, because of the additional burdens imposed upon consumers to use such devices. Accordingly, there is a need for a new method and system for using a biometric device to facilitate and authorize transactions with consumers and other parties, particularly transactions conducted over computer networks such as the Internet, in which the burdens imposed upon consumers and other parties to conduct such transactions are not increased.

SUMMARY OF THE INVENTION

[0006] In one aspect, the present invention provides a method for effecting a transaction between a person and a provider of goods or services over a computer network. The method includes establishing from a communication device a communication link over the computer network with the provider. The method also includes entering into the communication device information pertinent to effecting the transaction. The method further includes activating in conjunction with effecting the transaction a biometric device to generate a unique identification trait (UIT) associated with the person and, in response to this activating, automatically transmitting from the communication device over

the computer network to the provider both the information and a signal corresponding to the UIT.

[0007] In another aspect, the present invention provides a communication device for effecting a transaction between a person and a provider of goods or services over a computer network. The communication device includes a network connection device for establishing from the communication device a communication link over the computer network with the provider. The communication device also includes a computer input device for entering into the communication device information pertinent to effecting the transaction. The communication device further includes a biometric device for activating by the person in conjunction with effecting the transaction to generate a UIT associated with the person and a processor, responsive to this activating, for automatically causing the transmission from the communication device over the computer network to the provider of both the information and a signal corresponding to the UIT.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 illustrates a system for conducting secure transactions over a network in accordance with the present invention.

[0009] FIG. 2 illustrates a biometric device integrated into a communications device in accordance with the present invention.

[0010] FIG. 3 is a flow diagram of a method in accordance with the present invention.

[0011] FIG. 4 is a flow diagram of an alternative method in accordance with the present invention.

[0012] FIG. 5 is a flow diagram of a method for associating specific data files with specific unique identification traits of a person in accordance with the present invention.

[0013] FIG. 6 illustrates a system for using specific data files associated with specific unique identification traits of a person in accordance with the present invention.

[0014] FIG. 7 illustrates an alternative embodiment of a system for using specific data files associated with specific unique identification traits of a person in accordance with the present invention.

[0015] FIG. 8 illustrates a user's interface for a biometric device and a communications device in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] FIG. 1 illustrates a system 201 for conducting secure transactions over the Internet, or over other computer networks, in accordance with the present invention.

[0017] As shown in FIG. 1, consumer 200 uses one of a variety of communication devices 202 to connect to Internet 204 over links 218. Links 218 may be telephone lines, cable systems, optical systems, wireless systems, satellite systems,

or any other systems capable of transmitting information between a communication device 202 and a computer network. A communication device 202 may be any device for transmitting and receiving such information. A communication device 202 typically includes a central processing unit (CPU) and a network connection device, e.g., a network adapter card, a network interface card, a standard cable modem, a DSL modem, an ADSL modem, an ISDN modem, a cable modem or a wireless modem. A communication device 202 may be, e.g., a wireless device, such as a personal digital assistant (PDA), cell phone, satellite broadcasting set-top box or a portable computer with a wireless modem. On the other hand, a communication device 202 may be a wired device, such as a personal computer, server, point-of-sale terminal, ATM machine, cable set-top box or land-line telephone. In lieu of Internet 204, any network capable of providing communications between and among such devices may be employed.

[0018] Using a communication device 202, consumer 200 accesses a provider, e.g., provider 212, over links 218, Internet 204 and, e.g., link 220. Provider 212 may be any entity providing goods or services over Internet 204, e.g., consumer goods, electronic banking, movies, stock trading, news, information or any other goods or services. Other participants 214, such as individuals, institutions and other entities, also interact with provider 212, other providers

(not shown), consumer 200 and other consumers (not shown), over Internet 204. Bank 216 communicates with provider 212 over dedicated link 222 or link 230 and Internet 204. Bank 216 provides financial information, such as the verification of credit information, to provider 212 to assist provider 212 in conducting sales and other transactions.

[0019] In accordance with the present invention, a communication device 202 includes a biometric device 210. Biometric device 210 measures and analyzes a human characteristic, referred to herein as a unique identification trait (UIT). The UIT may be a fingerprint, retina pattern, iris pattern, scent pattern, voice pattern, DNA pattern, heat pattern, keystroke pattern, facial image or any other characteristic uniquely identifying an individual. Biometric device 210 compares an entered UIT of an individual against a copy of the UIT previously stored in a database 250 to authenticate the identity of the individual. The previously stored copy of the UIT normally is a digital representation of the UIT, and the comparison normally is performed by, e.g., a microprocessor, hard wired logic, ASIC or other digital processing device. Database 250 may be stored in a RAM, ROM, EEPROM, magnetic tape, floppy disk, optical disk or any other computer memory device associated with communication device 202. On the other hand, database 250 may be associated with provider 212, bank 216 or other participants 216 and connected

to communication device 202 through Internet 204. The comparison of an entered UIT against a stored UIT normally involves creating a digital representation of the entered UIT, comparing that digital representation with the UIT stored for that individual and, if a match occurs, generating a verification signal. Of course, analog techniques also may be employed for this process. Such biometric devices are well known to those skilled in the art.

[0020] As shown in FIG. 2, biometric device 210 may be integrated into a display cabinet associated with a communication device 202. Icon 212 provides a visual indication to a user that biometric device 210 should be activated in conjunction with completing a transaction. Biometric device 210 also may be integrated into a mouse, keyboard, case or display (using touch screen techniques) associated with a communication device 202. On the other hand, some components of biometric device 210 may be at provider 212, bank 216 or other participants 214 and connected to communication device 202 through Internet 204.

[0021] In accordance with the method of the present invention, a user, such as consumer 200, activates biometric device 210 in conjunction with conducting a transaction with provider 212 over Internet 204. This activation, however, does not increase the burdens imposed upon consumer 200 to conduct the transaction.

[0022] A flow diagram for conducting a transaction with a provider 212 of goods or services in accordance with the present invention is shown in FIG. 3. This example is equally applicable, however, to any entity conducting transactions with individuals or other entities over any other computer network.

[0023] Referring to FIG. 3, at action 300, consumer 200, using conventional methods, connects to provider 212 over Internet 204 using a communication device 202. At action 302, consumer 200 browses the website of provider 212 and selects desired goods for purchase. At action 304, consumer 200 notifies provider 212 of his or her selection of goods for purchase. This notification may occur, e.g., by clicking on an icon representing the goods, clicking on a picture of the goods or transmitting an appropriate message identifying the goods entered on a keyboard. At action 306, provider 212, in response, electronically transfers to consumer 200 a form requesting various personal and financial information to complete the transaction (e.g. name, address, quantity of goods, payment information, etc.). Provider 212 also requests that the identity of consumer 200 be verified through the transmission of a verification signal from biometric device 210.

[0024] In response, using communication device 202, consumer 200, at action 308, enters all of the necessary

personal and financial information into the form. At action 310, consumer 200 activates biometric device 210. For example, if biometric device 210 is a fingerprint analyzer, consumer 200 would then place his or her finger in or on the sensor for such a device. If the UIT generated by biometric device 210 matches the UIT for consumer 200 stored in database 250, a verification signal is generated and transferred to provider 212. With this signal, and without further action by consumer 200, all of the personal and financial information entered into the form by consumer 200 at action 308 also are transmitted to provider 212. This information is transmitted to provider 212 with the verification signal without consumer 200 clicking on an icon, pressing a key on a keyboard or taking any other additional action to initiate this transmission. The step of verification using biometric device 200, therefore, does not add a step to the ordering process. At action 312, provider 212 receives the verification signal, verifies the personal and financial information transmitted, executes the order and notifies consumer 200 that the transaction is complete.

[0025] The verification signal may indicate only that the identity of consumer 200 has been verified. On the other hand, the verification signal may comprise a unique verification code, such as a number, password or other indicia uniquely associated with consumer 200. This verification code

may be transmitted in encrypted or non-encrypted format. If a verification code is transmitted to provider 212, provider 212, in addition to verifying the personal and financial information of consumer 200, also may verify this code. For example, provider 212 may refer to a database maintained by it, or another entity, containing a compilation of such verification codes and the identity of the individuals to whom they correspond. Provider 212 then can determine whether the code transmitted is in this database and, if so, whether the identity of the individual to whom the code corresponds is consumer 200.

[0026] In the alternative, in lieu of a verification signal or a verification code, biometric device 210, upon activation, may transfer to provider 212, in addition to all of the personal and financial information entered into the form, the generated UIT. In this case, provider 212 would compare the generated UIT against the UITs stored in database 250 to verify the identity of consumer 200.

[0027] The method described above provides, therefore, an enhanced level of security for transactions conducted over the Internet, or over other computer networks, without imposing increased burdens upon consumers or other individuals for completing such transactions.

[0028] An alternative method in accordance with the present invention is shown in FIG. 4. As shown in this figure, at

action 400, before contacting a provider, such as provider 212, consumer 200 enters his or her personal and financial information into a file of a database, such as database 250, associated with the biometric device. This information may include the consumer's name, address, social security number, sex, date of birth, credit card number, password, bank name, shipping address, billing address, etc. This file is associated with a UIT of consumer 200 and, in addition, also may be associated with other information, e.g., a particular provider or providers, a particular credit card number, etc. As discussed below in connection with FIG. 5, database 250 may include a number of such files, each associated with a different UIT of consumer 200 or other individuals. Each of these files also may be further associated with other information, e.g., a different credit card number, a different provider or group of providers, etc.

[0029] Referring again to FIG. 4, at action 402, using communication device 202, consumer 200 connects to provider 212 using conventional techniques. At action 404, consumer 200 browses the website of provider 212 and selects particular goods or services for purchase. At action 406, consumer 200 notifies provider 212 of his or her desire to purchase particular goods, e.g., by clicking on a button, icon or picture of the goods, transmitting a message entered on a keyboard, etc. At action 408, provider 212 transfers an order

form to communication device 202 and requests consumer 200 to provide all necessary personal and financial information to complete the transaction. Provider 212 also requests that consumer 200 provide a verification signal or a verification code.

[0030] In response to this request, consumer 200, at action 410, activates biometric device 210. At action 412, a determination is made of whether the generated UIT matches any of the UITs associated with the files in database 250. If no match is found, a message is displayed on the display of communication device 202 at action 416 telling consumer 200 that verification of his or her identity was not successful and that he or she may reactivate biometric device 210 again to again attempt verification. On the other hand, if at action 412, the UIT generated matches one of the UITs associated with the files in database 250, then, at action 414, without further action by consumer 200, the personal and financial information in the file associated with the UIT are automatically entered into the form, and the completed form and verification signal or verification code are transmitted to provider 212. If several files in database 250 correspond to the same UIT but different providers, then the file corresponding to provider 212 is transmitted.

[0031] At action 418, provider 212 verifies the personal information, financial information and, if transmitted, the

verification code. At action 420, if verification is successful, provider 212 executes the transaction and notifies consumer 200 that the transaction is complete.

[0032] FIG. 5 is a flow diagram of the steps for creating a group of files in database 250 in accordance with the method of FIG. 4. Each of these files is uniquely identified by a particular UIT of consumer 200 and perhaps also by particular UITs of other individuals. Each of these files also may be further uniquely identified by a particular provider or providers, credit card number or other information.

[0033] As shown in FIG. 5, consumer 200, using a keyboard or other computer input device associated with communication device 202, enters into a file of database 250 personal information, financial information and various other information for conducting transactions with provider 212 or other providers. This other information may include information pertinent to provider 212 or other providers, e.g., a particular pass code, sign-on routine, etc. At action 502, consumer 200 is asked whether the files should be associated with a particular provider or providers. If no such association is desired, consumer 200 moves to action 506. On the other hand, if such an association is requested, consumer 200 moves to action 504 where, again using a keyboard or other computer input device associated with communications device, he or she enters information identifying the

particular provider or providers with which the file is to be associated. Consumer 200 then moves to action 506 where he or she activates biometric device 210. This activation causes a UIT to be generated and associated with the file. Consumer 200, at action 508, then is asked whether additional files for database 250 are to be created. If additional files are to be created, consumer 200 returns to action 500 where the information for the next file is entered. If no additional files are to be created, the program terminates.

[0034] FIGS. 6 and 7 illustrate the use of files created in accordance with the method illustrated in FIG. 5 in executing transactions over Internet 204 using communication device 202.

[0035] In the first example, as shown in FIG. 6, database 250 comprises a number of such files, and biometric device 210 comprises fingerprint analyzer 600. Each of the files is associated with a different fingerprint of consumer 200. For example, UIT 1, which is associated with file 1, may be the fingerprint of the right thumb of consumer 200, UIT 2, which is associated with file 2, may be the fingerprint of the right index finger of consumer 200, etc. Therefore, if in conjunction with executing a transaction with provider 212, consumer 200 is requested to transmit a verification signal or verification code and the information contained in file one, consumer 200 simply places his or her right thumb on sensor 602 of fingerprint analyzer 600. The verification signal or

code, and the information contained in file one, then are transmitted automatically to provider 212 without further action by consumer 200. If consumer 200 is requested during a transaction with provider 212 to transmit a verification signal or verification code and the information contained in file two, consumer 200 simply places his or her right index finger on sensor pad 602. The verification signal or code, and the information contained in file two, then are transmitted automatically to provider 212 without further action by consumer 200.

[0036] In addition to a UIT, each of the files may be further associated with a particular provider or providers. For example, a first file may be associated with UIT 1 and provider 212, and a second file may be associated with UIT 1 and another provider. The identity of the particular provider with which communication device 202 is in communication during a transaction normally is known to communication device 202 under conventional communication protocols. Therefore, if in conjunction with executing a transaction with provider 212 consumer 200 is requested to transmit a verification signal or verification code and the information contained in the first file, when consumer 200 enters UIT 1, e.g., by placing his or her right thumb on sensor 602, the verification signal or code and the information in only the first file automatically are transmitted to provider 212.

[0037] Rather than each of these files containing all of the personal and financial information necessary to complete a transaction, subsets of this information may be included in the files. For example, as shown in FIG. 7, a first file associated with UIT 1 may contain only a final authorization signal for a transaction, a second file associated with UIT 2 may contain an account name, a third file associated with UIT 3 may contain an account number, a fourth file associated with UIT 4 may contain a first shipping address and a fifth file associated with UIT 5 may contain a second shipping address. If during a transaction with provider 212 or another provider, therefore, consumer 200 is requested to transmit a verification signal or a verification code and an account name, consumer 200 simply enters UIT 2, e.g., places his or her right index finger on sensor 602 of fingerprint analyzer 600. If consumer 200 merely wishes to submit with the verification signal or verification code a final authorization for the transaction, consumer 210 simply enters UIT 1, e.g., places his or her right thumb on sensor 602. Of course, if additional biometric devices are employed, such as retinal scanners, voice recognition devices, etc., additional files can be stored in database 250 in this manner or as shown in FIG. 6, and each of these additional files may be associated with the particular UITs of consumer 200 or other individuals corresponding to these devices.

[0038] FIG. 8 illustrates an example of a user's interface for biometric device 210 and communication device 202 for operation in accordance with the present invention. In this example, communication device 202 typically is, e.g., a point-of-sale terminal or a wireless communication device, such as a PDA.

[0039] As shown in this figure, display 804 of communication device 202 provides various prompts and instructions to consumer 200 for completing a transaction. Fingerprint analyzer 814 is integrated into case 802 of communication device 202. LEDs 810 and 812 provide signals when biometric device 210 is activated to indicate whether verification of consumer 200 is successful (OK) or unsuccessful(NG). Icons 806 and 808 appearing in display 804 provide signals to consumer 202 to assist him or her in completing a transaction. If display 804 includes a touch-sensitive screen, responses to these signals may be transmitted by touching these icons. In the alternative, responses may be transmitted using a mouse, keyboard or other computer input device. Also, in lieu of LEDs 810 and 812, and icons 806 and 808, audible indicators may be used.

[0040] As illustrated, communication device 202 in this example may be used to pay a particular provider a sum of money for goods, e.g., groceries. As part of this transaction, a question appears in display 804 asking consumer

200 whether the amount of the payment should be submitted. Consumer 200 also is told that this submission can be effected by activating biometric device 210. If consumer 200 wishes to make this payment, consumer 200 simply places his or her finger on the sensor associated with fingerprint analyzer 814. If the generated UIT matches the UIT for consumer 200 stored in database 250, LED 810 is lighted to inform consumer 200 that verification of his or her identity was successful. On the other hand, if the generated UIT does not match the UIT for consumer 200 stored in the database 250, LED 812 is lighted to inform consumer 200 that verification of his or her identity was not successful. If the verification was successful, a verification signal or a verification code are transmitted with a signal authorizing the making of this payment. On the other hand, if consumer 200 wishes to cancel submission of the payment, he or she touches icon 806, if display 804 is touch sensitive, or otherwise responds to this icon. Prior to submission, icon 808 remains lighted until the sensor associated with fingerprint analyzer 814 is activated. Upon activation of fingerprint analyzer 814, this icon goes dark. If submission of the payment is to be made without verification by the biometric device, consumer 200 may simply touch icon 808 to authorize this payment, again assuming display 804 is touch sensitive.

[0041] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.